(12) UK Patent Application (19) GB (11) 2 136 175 A

(43) Application published 12 Sep 1984

(21) Application No 8405950

(22) Date of filing 7 Mar 1984

(30) Priority data

(31) 472609 (32) 7 Mar 1983 (33) US

(51) INT CL³
H03K 13/24 G06F 15/00

(52) Domestic classification
G4A AP

(56) Documents cited
None

(58) Field of search
G4A

(71) Applicant
Atalla Corporation, (USA—California),
2363 Bering Drive, Sane Jose, California 95131,
United States of America

(72) Inventor
Martin M. Atalla

(74) Agent and/or address for service
Peter A. Oliver, 8 Coombe Close, Frimley, Surrey,
GU16 5DZ

(54) File Access Security Method and Means

(57) An improved file access security technique and associated apparatus 9 accesses data which is stored at 17 in encrypted form under one encryption key and re-stores the data re-encrypted under another encryption key, and produces at 19 a record of each access and data re-encryption both as the control source of encryption keys for access and re-entry of encrypted data and as a secured audit record of users that had access to each file.

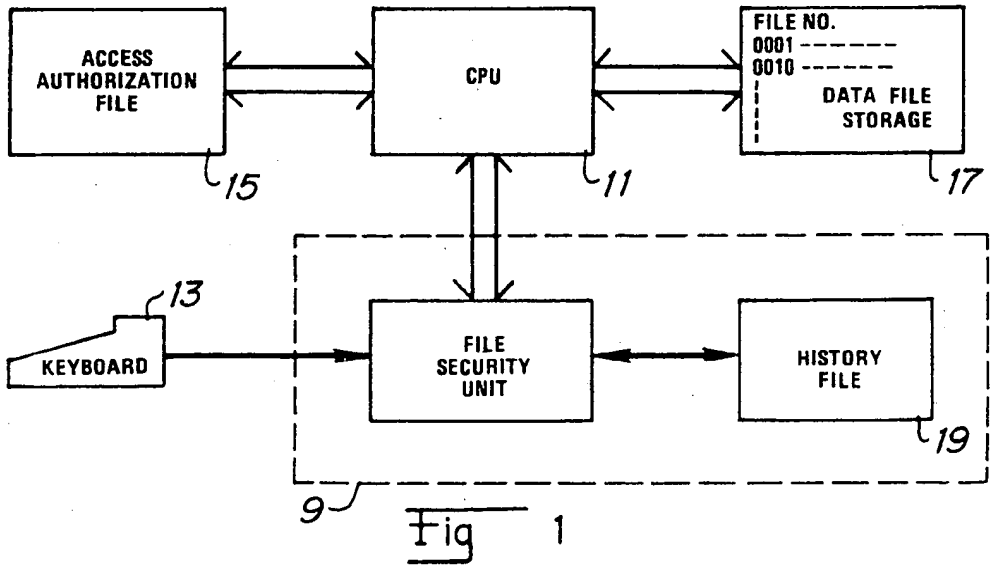

Fig 1

GB 2 136 175 A

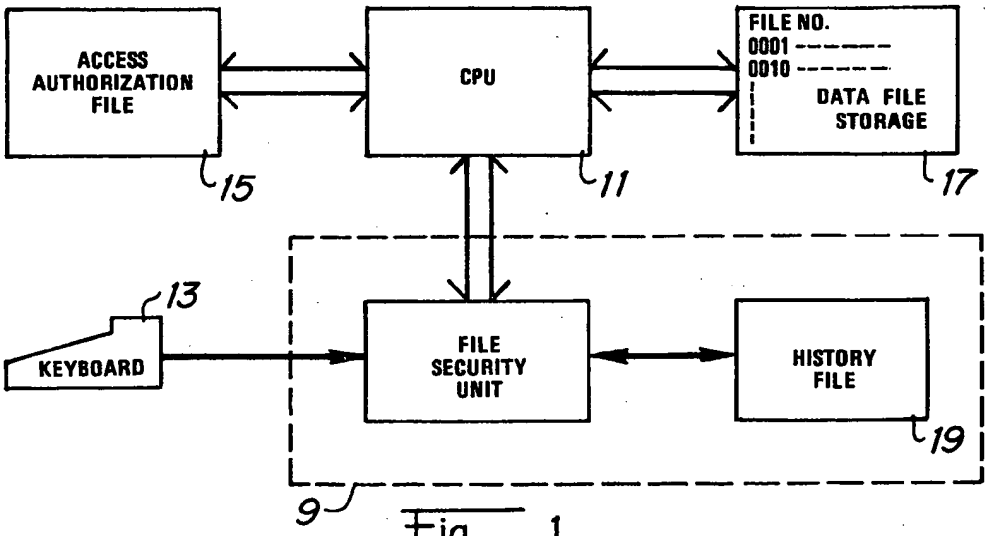
ACCESS AUTHORIZATION FILE
15
CPU
11
FILE NO.
0001
0010
DATA FILE STORAGE
17
13
KEYBOARD
FILE SECURITY UNIT
HISTORY FILE
19
9

Fig 1

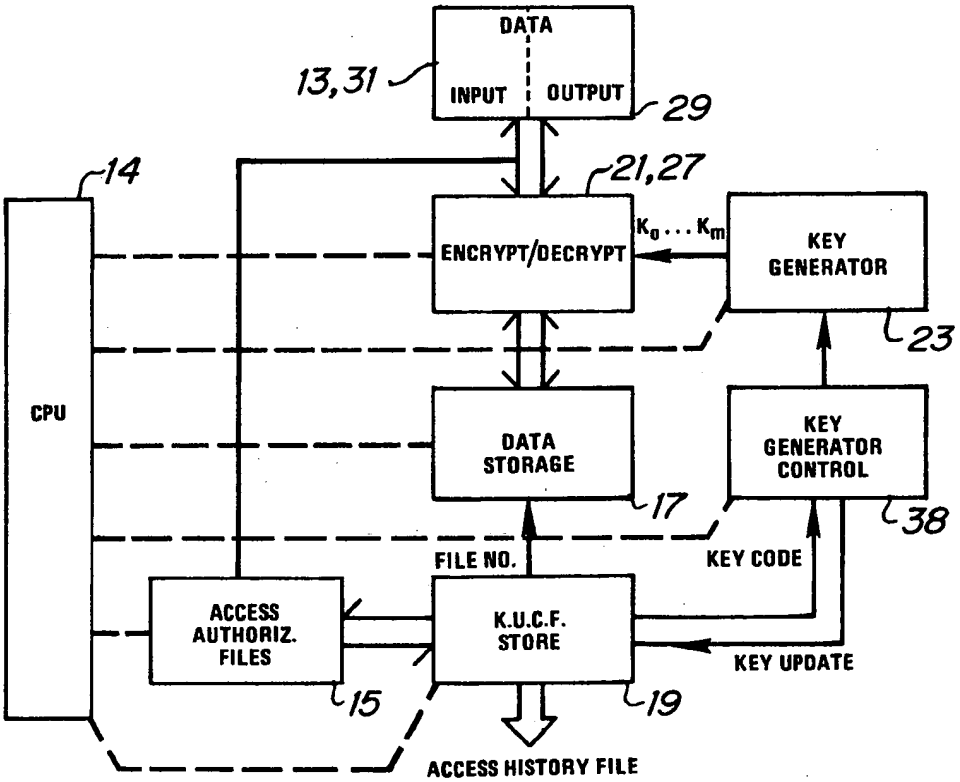
DATA
13,31
INPUT
OUTPUT
29
14
21,27
ENCRYPT/DECRYPT
$K_0 \ldots K_m$
KEY GENERATOR
23
CPU
DATA STORAGE
17
KEY GENERATOR CONTROL
38
FILE NO.
KEY CODE
ACCESS AUTHORIZ. FILES
15
K.U.C.F. STORE
19
KEY UPDATE
ACCESS HISTORY FILE

Fig 3

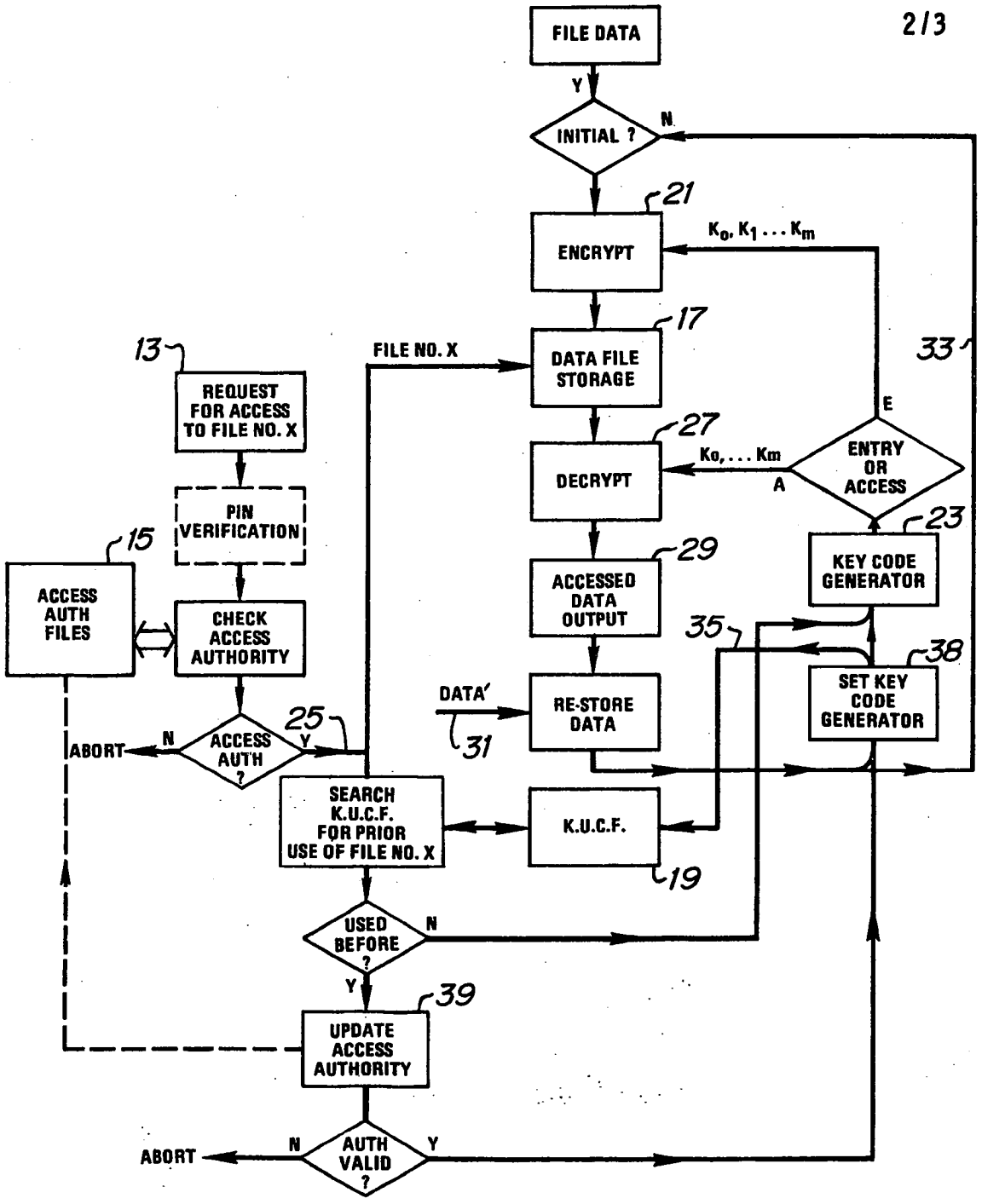
FILE DATA
Y
INITIAL ?
N
21
ENCRYPT
$K_0, K_1 \ldots K_m$
17
DATA FILE STORAGE
FILE NO. X
13
REQUEST FOR ACCESS TO FILE NO. X
PIN VERIFICATION
15
ACCESS AUTH FILES
CHECK ACCESS AUTHORITY
ABORT
N
ACCESS AUTH ?
Y
25
SEARCH K.U.C.F. FOR PRIOR USE OF FILE NO. X
K.U.C.F.
19
USED BEFORE ?
N
Y
39
UPDATE ACCESS AUTHORITY
ABORT
N
AUTH VALID ?
Y
27
DECRYPT
$K_0, \ldots K_m$
E
A
ENTRY OR ACCESS
33
23
KEY CODE GENERATOR
29
ACCESSED DATA OUTPUT
35
38
SET KEY CODE GENERATOR
DATA'
31
RE-STORE DATA

Fig 2

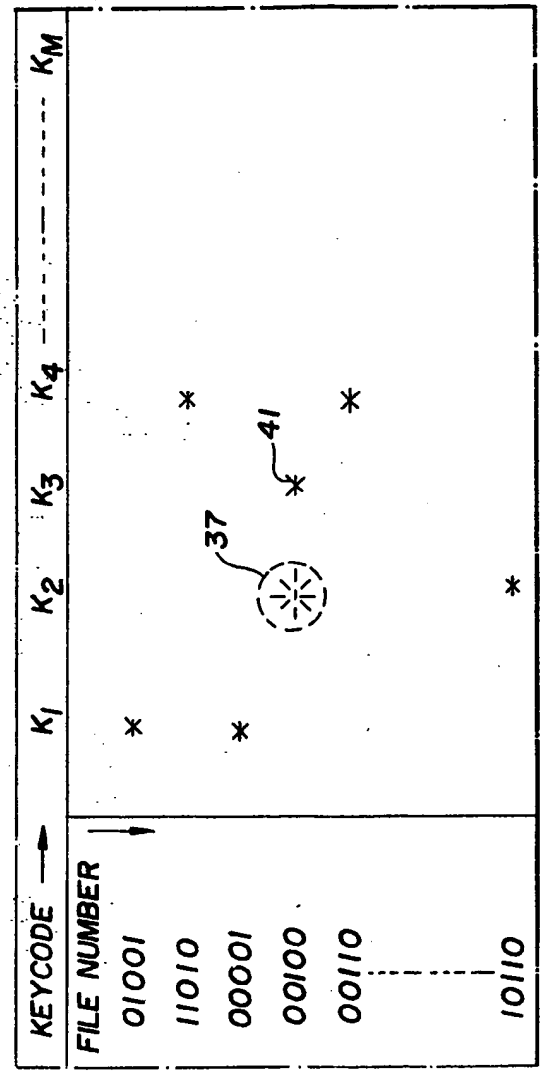
KEYCODE
FILE NUMBER
K_1
K_2
K_3
K_4
K_M
01001
11010
00001
00100
00110
10110
37
41

FIG. 4

SPECIFICATION

File Access Security Method and Apparatus

This invention is concerned with a method of and apparatus for securing data files in storage.

Many known computer-controlled operations on secured data files require verification of the identity of an individual seeking to access a file before the data (usually in encrypted form) can be accessed (see, for example, U.S. Patents 3,938,091, 3,587,051, 3,611,293 and 4,198,619). In addition, many known record-securing schemes including those associated with credit cards, require verification of both the authority of the using individual and the authenticity of the data in the record, to protect against unauthorized users and against counterfeit or duplicate records. Schemes of this type are disclosed in U.S. Patents 4,304,990, 4,328,414 and 4,357,429.

One disadvantage associated with computer-controlled security schemes of these types is that there is typically no indication left on file of who gained access to a secured record.

The present invention provides a method of securing data files in storage against unauthorized access, the method comprising the steps of encrypting file data as a selected logical combination thereof with an initial one of a plurality of encryption key codes to produce file data in encrypted form for storage at selected file address locations, establishing a record of accesses to each selected file address location and the one of the plurality of encryption key codes with which the file data at the address location is encrypted, processing a request for access to file data at a selected file address location by determining from the record the number of prior accesses thereof and the encyrption key code associated therewith, decrypting file data at the selected file address location using said associated encryption key code, re-encrypting file data for said selected file address location using a new one of said plurality of encryption key codes in said selected logical combination, storing the newly re-encrypted file data at the accessed file address location, and modifying the record to indicate an additional access to the selected file address location and the new encryption key code associated therewith.

In performing a method as set forth in the last preceding paragraph, it is preferred that in carrying out the step of decrypting, file data at a selected filed address location is decrypted using said initial encryption key code in response to determination from the record that said selected file address location was not previously accessed.

A method as set forth in either one of the last two immediately preceding paragraphs may further comprise the additional steps of establishing a file of user access authorizations, and prior to accessing a selected file address location, determining the authorization status of a user to gain access to the selected file address location.

A method as set forth in the last preceding paragraph may further comprise the additional step of selectively altering the access authorization of a user to gain subsequent access to the selected file address location in response to re-encryption of the file data for storage at the selected filed address location.

A method as set forth in any one of the last four immediately preceding paragraphs may further comprise the steps of reinitializing all the file data by decrypting the file data at each selected file address location using the encryption key code thereof determined from the record, and re-encrypting the file data at each such file address location using a new initial one of a plurality of key codes.

In performing a method as set forth in the last preceding paragraph, it is preferred that in carrying out the reinitialization step, the file data at any file address location which is not indicated in the record to have been accessed previously is decrypted using the initial encryption key code.

The present invention also provides apparatus for securing data filed in storage against unauthorized access, comprising storage means for storing file data in encrypted form at selectable file address locations, encryption means for supplying encrypted file data to a selected file address location as the logical encoding combination of file data and an encryption key signal applied thereto, generator means for applying selected encryption key signals to the encryption means, record means for producing indication of selected file address locations and key code signals associated with encryption of file data stored therein, circuit means responsive to indentification of a selected file address location for determining from said record means the encryption key signal associated therewith for setting the generator means to supply the associated encryption key signal, decryption means disposed to receive encryption key signals from the generator means and encrypted file data from the storage means and operable in accordance with said logical encoding combination to decrypt the file data at said selected file address location, and means operable upon the decrypted file data for altering the generator means to supply a new encryption key signal for re-storing the file data at the selected file address location newly encrypted with a new encryption key signal, said means altering the record means to produce an indication of the new encryption key signal associated with file data in the selected file address location.

In apparatus as set forth in the last preceding paragraph, it is preferred that said circuit means is responsive to the indication in said record means that a selected file address location was not previously accessed for setting said generator means to supply the initial encryption key signal to the decryption means.

Apparatus as set forth in either one of the last two immediately preceding paragraphs may further comprise access record means for storing data representative of the authorization of users to selectively access file data in said storage means, and means disposed to receive identification data from a user, and coupled to said circuit means for inhibiting the generator means from supplying an encryption key signal to said decryption means for an unauthorized, identified user.

Apparatus as set forth in the last preceding paragraph may further comprise means responsive to re-storing of file data at the selected file address location newly encrypted with a new encryption key signal for altering the identified user's authorization in said access record means to access said selected file address location.

Apparatus as set forth in the last preceding paragraph but three may further comprise initializing means coupled to said generator means, said encryption means and decryption means and to said record means for setting the generator means to selectively decrypt file data in each file address location using the encryption key signals from said generator means established from the record means for each such file address location, and for re-encrypting the decrypted file data for each file address location using a new initial encryption key signal for re-storage at the respective file address location.

In apparatus as set forth in last preceding paragraph, it is preferred that said initializing means responds to indication from said record means of no previous access to a selected file address locations for decrypting file data therein in using an initial encryption key signal and for re-encrypting the decrypted file data using a new initial encryption key signal to re-store the newly encrypted file data at the respective file address location.

The present invention further provides a file access record produced by a process comprising the steps of storing at selected file address locations file data that is encrypted as the logical combination of file data and selected ones of a plurality of encryption key signals; decrypting file data at a selected file address location using the encryption key signal associated therewith in accordance with said logical combination, re-encrypting the decrypted file data as a logical combination thereof and a new encryption key signal for re-storing at the corresponding file address location, and producing said file access record as the compilation at least of the number of times each selected file address location was decrypted and information indicative of the encryption key signals with which the file data at each selected file address location was reencrypted and re-stored therein.

In accordance with the preferred embodiment of the present invention, a dynamic record of encryption control keys used to gain access initially and at all subsequent occasions to secured encrypted files is generated both as an active element of the accessing scheme and as a secured, historic record for audit purposes of all accesses to encrypted files. In addition, substitutions of outdated files are prevented once a file is accessed, even merely for display without alteration, so that a file once accessed, and therefore with its security compromised, can be resecured against duplication, substitition, and re-use. Schemes of this type are particularly useful in banking and funds-transfer operations where proper access initially to an account file, for example, to effect a withdrawal of funds, must thereafter be carefully controlled to avoid such disastrous practices as multiple replication of the same operation coupled with substitution of the original balance back into the file. Further, the historic record of accesses to files produced by the present invention constitutes an audit record in encrypted form of such accesses.

There now follows a detailed description which is to be read with reference to the accompanying drawings of a method and apparatus according to the present invention; it is to be clearly understood that this method and apparatus have been selected for description to illustrate the invention by way of example and not by way of limitation.

In the accompanying drawings:

Figure 1 is a pictorial block diagram showing one application of the apparatus of the present invention;

Figure 2 is a flow chart illustrating the operation of the apparatus of Figure 1;

Figure 3 is a block diagram of the illustrated embodiment of the present invention; and

Figure 4 is a chart illustrating the formation and operation of the key usage control file according to the present invention.

Referring now to Figure 1, there is shown a pictorial block diagram of the present invention illustrating the addition of an access-securing module 9 to a typical computer system comprising a central-processing unit 11, keyboard controller 13, and memory means 15, 17 for storing files. The memory means 15, 17 may use any conventional form of storage technology such as semiconductor memory, magnetic memory in core, crystal, disc, drum, or tape form, and any combinations thereof, to provide means 17 for storing the data to which access is to be controlled, and to provide means 15 for storing access authorization information about individuals and entities that may access the stored data means 17. The keyboard controller 13 provides manual-entry access to the computer system in conventional manner and is representative of other computer-accessing schemes such as by another computer system, and the like.

In accordance with the present invention, such a typical computer system is modified to include the access-securing module 9 which operates with the computer system to progressively re-encrypt the data in storage in memory means 17 each time a file is accessed, and optionally to

update the access authorization information in storage in the memory means 15 in response to authorizations granted, and to generate historic files in encrypted form of the encryption keys used to decrypt and re-encrypt each file accessed from the memory means 17. In addition, the module 9 operates in a controlled reinitialization mode to restore all files in the memory means 17 to a new, standard encryption key after numerous accesses of files in the memory means 17 have been authorized. The number of accesses before requiring reinitialization is determined by the memory capacity in the module 9.

Referring now to Figures 2 and 3 in addition to Figure 1, there are shown a flow chart and a block diagram, respectively, illustrating the operation of the system of Figure 1 under control of a central processing unit 11. In operation, a person or entity, R, requesting access to a particular file may enter personal identification numbers, information about the particular file, and the like, via the keyboard controller 13. Optionally, a personal-identity verification routine may be performed in conventional manner (as disclosed, for example, in U.S. Patent 3,938,091 or 4,198,619) and the access-authorization files in the memory means 15 may be searched for authorization to access the requested file. All such files in memory means 17 are initially encrypted with an initial key code, K_0, in a conventional manner (for example, using the *D*ata *E*ncryption *S*tandard module available from the *N*ational *B*ureau of *S*tandards) by encrypting the file data in an encryption module 21 with key code, K_0, from a key code generator 23.

With authorization established 25, the particular file #X may be accessed, but decrypting the file #X requires the correct key code. For this purpose, a key-usage control file 19, later described herein in detail, is searched to determine if the file #X was previously accessed. The conditions of prior access, namely, that it was, or it was not previously accessed, are possible. If it was not, then file #X will not appear in the key-usage control file, an indication that it appears in storage provided by the memory means 17 encrypted with the initial key code, K_0. The key code generator 23 is capable of generating a sequence of different key codes K_0, K, K_2, K_3 . . . K_n and is set to supply key code K_0 to a decryption module 27 (which, of course, may be the same type of DES module, or may be the same module, as the encryption module 21). The requested file #X may therefore be decrypted in conventional manner using the key code K_0 to provide accessed data 29 in clear text. The data is then returned to storage, either without or with new data modifications 31 that reflect a data-oriented transaction such as sale, deposit, withdrawal, or the like, and is re-stored in encrypted form using a new key code K_1. This is accomplished by resetting 38 the key code generator 23 to supply the key code K_1 to the encryption module 21 and returning the data 33 with or without modifications for encryption in the module 21 with the key code K_1. In addition, the key-usage control file 19 is updated to reflect that the file #X was accessed and now resides in storage newly-encrypted with the new key code K_1 in the sequence. Further, the access-authorization in the memory means files 15 may be updated optionally to inhibit further access to file #X by user R, for example, to inhibit R's further access until a "new date", or until accessed by another user, or the like. Subsequent access to file #X by user R, if continuously authorized, or by any other user must be via decryption with the key code K_1.

If file #X was previously accessed, then the key-usage control file 19 will contain the entry of file #X having been previously accessed and returned to storage encrypted with a new key code K_1, K_2 . . . K_n, depending upon the number of previous accesses to file #X. Thus, with reference to the chart of Figure 4 which illustrates the typical entries in the key-usage control file 19, if file #X is file #00100, then the previous accesses to this file resulted in its being re-stored encrypted with key code K_2 (at entry 37). The search of the key-usage control file 19 thus indicates that file #00100 was previously accessed twice and now requires decryption with key code K_2. If authorization of the requesting user is still valid 39, then the key code generator 23 is set to supply the key code K_2 to the decryption module 27 in order to furnish the data in this file in clear text 29. Re-storing the data from this file in modified or unmodified form is accomplished by resetting 38 the key code generator 23 to supply the key code K_3 (entry 41 in Figure 4) to the encryption module 21 for encryption therein of the returned data with the new key code K_3. All retrievals of data in storage in the memory means 17 may be by destructive read of information in the addressed file so that data for restoring therein may be written in in the newly-encrypted form. After numerous accesses to files in storage in the memory means 17, the key-usage control file 19 will typically include entries as illustrated in Figure 4. Such a file optionally may also include codes to identify the particular users who gained access to each file. The file 19 thus provides an audit record of the accesses to the files in the memory means 17. In addition, the key-usage control file 19 is in encrypted form since it neither reveals the data in storage in the memory means 17 nor the actual key codes K_1 . . . K_n (only generated by the generator 23) required to decrypt the data in storage. Further, the key codes K_0 . . . K_n which serve as file-protect codes can be generated internally in conventional manner, for example, by a random-number generator 23 and therefore need not be known to anyone.

After numerous accesses to the data in storage 17 which approaches the limit of the sequence of key codes for any particular file, or on a periodic basis, the entire collection of files in storage 17 may be re-encrypted with a new initial key code K_0' of a sequence of new key codes K_0', K_1' . . . K_n'

using the apparatus illustrated in Figure 3 under control of the central processing unit 14. However, since the files in storage 17 are encrypted with different key codes, the key-usage control file 19 must be consulted to determine which key code to use to decrypt the data in each file for re-encryption with a new initial key code K_0'. After completion of this reinitialization mode of operation, the key-usage control file 19 for the sequence of key codes $K \ldots K_n$ may be retired to serve as an historic record of access to the data in storage 17 without compromising the security of the system or of the data in storage 17 under new encryption codes.

CLAIMS

1. A method of securing data files in storage against unauthorized access, the method comprising the steps of:

encrypting file data as a selected logical combination thereof with an initial one of a plurality of encryption key codes to produce file data in encrypted form for storage at selected file address locations;

establishing a record of accesses to each selected file address location and the one of the plurality of encryption key codes with which the file data at the address location is encrypted;

processing a request for access to file data at a selected file address location by determining from the record the number of prior accesses thereof and the encryption key code associated therewith;

decrypting file data at the selected file address location using said associated encryption key code;

re-encrypting file data for said selected file address location using a new one of said plurality of encryption key codes in said selected logical combination;

storing the newly re-encrypted file data at the accessed file address location; and

modifying the record to indicate an additional access to the selected file address location and the new encryption key code associated therewith.

2. A method according to claim 1 wherein, in carrying out the step of decrypting, file data at a selected file address location is decrypted using said initial encryption key code in response to determination from the record that said selected file address location was not previously accessed.

3. A method according to either one of claims 1 and 2 comprising the additional steps of establishing a file of user access authorizations; and prior to accessing a selected file address location

determining the authorization status of a user to gain access to the selected file address location.

4. A method according to claim 3 comprising the additional step of selectively altering the access authorization of a user to gain subsequent access to the selected file address location in response to re-encryption of the file data for storage at the selected file address location.

5. A method according to any one of the preceding claims and further comprising the steps of:

reinitializing all the file data by decrypting the file data at each selected file address location using the encryption key code therefor determined from the record; and

re-encrypting the file data at each such file address location using a new initial one of a plurality of key codes.

6. A method according to claim 5, wherein, in carrying out the reinitialization step the file data at any file address location which is not indicated in the record to have been accessed previously is decrypted using the initial encryption key code.

7. A method of securing data files in storage against unauthorized access substantially as hereinbefore described with reference to the accompanying drawings.

8. Apparatus for securing data files in storage against unauthorized access, comprising:

storage means for storing file data in encrypted form at selectable file address locations;

encryption means for supplying encrypted file data to a selected file address location as the logical encoding combination of file data and an encryption key signal applied thereto;

generator means for applying selected encryption key signals to the encryption means;

record means for producing indication of selected file address locations and key code signals associated with encryption of file data stored therein;

circuit means responsive to identification of a selected file address location for determining from said record means the encryption key signal associated therewith for setting the generator means to supply the associated encryption key signal;

decryption means disposed to receive encryption key signals from the generator means and encrypted file data from the storage means and operable in accordance with said logical encoding combination to decrypt the file data at said selected file address location; and

means operable upon the decrypted file data for altering the generator means to supply a new encryption key signal for re-storing the file data at the selected file address location newly encrypted with a new encryption key signal, said means altering the record means to produce an indication of the new encryption key signal associated with file data in the selected file address location.

9. Apparatus according to claim 8 wherein said circuit means is responsive to the indication in said record means that a selected file address location was not previously accessed for setting said genrator means to supply the initial encryption key signal to the decryption means.

10. Apparatus according to either one of claims 7, 8 and 9 and further comprising:

access record means for storing data representative of the authorization of users to selectively access file data in said storage means; and

means disposed to receive identification data from a user, and coupled to said circuit means for inhibiting the generator means from supplying an encryption key signal to said decryption means for an unauthorized, identified user.

11. Apparatus according to claim 10 comprising means responsive to re-storing of file data at the selected file address location newly encrypted with a new encryption key signal for altering the identified user's authorization in said access record means to access said selected file address location.

12. Apparatus according to claim 8 comprising initializing means coupled to said generator means, said encryption means and decryption means and to said record means for setting the generator means to selectively decrypt file data in each file address location using the encryption key signals from said generator means established from the record means for each such file address location, and for re-encrypting the decrypted file data for each file address location using a new initial encryption key signal for restorage at the respective file address location.

13. Apparatus according to claim 12 wherein said initializing means responds to indication from said record means of no previous access to a selected file address location for decrypting file data therein in using an initial encryption key signal and for re-encrypting the decrypted file data using a new initial encryption key signal to re-store the newly encrypted file data at the respective file address location.

14. Apparatus for securing data files in storage against unauthorized access substantially as hereinbefore described with reference to the accompanying drawings.

15. A file access record produced by a process comprising the steps of:

storing at selected file address locations file data that is encrypted as the logical combination of file data and selected ones of a plurality of encryption key signals;

decrypting file data at a selected file address location using the encryption key signal associated therewith in accordance with said logical combination;

re-encrypting the decrypted file data as a logical combination thereof and a new encryption key signal for restoring at the corresponding file address location; and

producing said file access record as the compilation at least of the number of times each selected file address location was decrypted and information indicative of the encryption key signals with which the file data at each selected file address location was re-encrypted and re-stored therein.

Printed in the United Kingdom for Her Majesty's Stationery Office, Demand No. 8818935, 9/1984. Contractor's Code No. 6378.
Published by the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.